Simulazione di infrastrutture critiche eterogenee e interdipendenti

Manuela Aprile, Stefano De Porcellinis, Roberto Setola, Stefano Panzieri

Nei paesi sviluppati le infrastrutture critiche, come quelle adibite alla produzione energetica, alla gestione delle acque, le reti di approvvigionamento, le reti di telecomunicazione ecc., risultano sempre più mutuamente dipendenti. A seguito di questo fenomeno, vulnerabilità nuove e molto pericolose possono affliggere l'intero sistema infrastrutturale: un guasto (failure), accidentale o doloso (per esempio un attacco terroristico), può infatti diffondersi in modo impredicibile, amplificato nelle sue conseguenze negative e tale da colpire imprevedibilmente un vasto insieme di utenti.

A causa della complessità e della interdipendenza che caratterizzano spesso il sistema composto dalle differenti infrastrutture, per analizzare le vulnerabilità gli approcci analitici sembrano essere in molti casi eccessivamente semplificati, mentre simulazioni "brute-force" soffrono della necessità di acquisire troppe informazioni dettagliate e spesso sensibili.
Per superare parzialmente questi svantaggi, in questo articololo proponiamo un approccio per modellare infrastrutture interdipendenti che, sulla base di informazioni principalmente qualitative, conduca a una simulazione in grado di supportare l'analisi della propagazione di *failure* e del decadimento globale delle performance.
Il simulatore, denominato Cisia, adotta una rappresentazione modulare e sufficientemente astratta dei differenti componenti delle infrastrutture tale da permettere descrizioni consistenti a partire anche da dati incompleti e generici, quali quelli spesso acquisibili dagli *stakeholder*. Una parte importante del lavoro di modellazione delle infrastrutture è stata riservata alla rappresentazione delle dipendenze e delle interdipendenze tra le loro componenti, essendo queste la principale causa dei comportamenti complessi e imprevedibili oggetto della nostra analisi. Secondo la rappresentazione adottata, ogni componente interagisce con gli altri attraverso una moltitudine di meccanismi, che codificano differenti concetti di prossimità. Il simulatore è stato utilizzato per analizzare, in una rappresentazione semplificata, gli effetti, in un'area urbana di Roma, in presenza di un failure nel sistema di trasmissione dall'energia elettrica.

Introduzione

Nei Paesi sviluppati, la qualità della vita di larghi segmenti della popolazione dipende da un gran numero di infrastrutture tecnologiche, quali quelle per la produzione, la trasmissione e la distribuzione di energia elettrica, le reti delle telecomunicazione, le reti idriche, le reti di approvvigionamento, i trasporti (aerei, ferroviari, marini, stradali), i servizi bancari e finanziari, ecc. A causa della loro rilevanza, queste infrastrutture sono generalmente indicate come Infrastrutture Critiche perchè "se danneggiate o distrutte, avrebbero un serio impatto sulla salute, la sicurezza, la salvaguardia, il benessere economico dei cittadini e sull'efficace funzionamento dei governi". [1]
Negli ultimi anni, per ragioni economiche, sociali, politiche ed economiche, si è osservato un rapido cambiamento nelle strutture organizzative, operative e fisiche di queste infrastrutture. Infatti, per ridurre i costi, migliorare l'efficienza e fornire servizi innovativi, appoggiandosi sempre più alle tecnologie ICT molte infrastrutture sono diventate estremamente interoperabili. Inoltre, per operare in modo efficace e redditizio nel mercato globale e in assenza di privilegi monopolistici, gli *stakeholder* tendono a concentrarsi sempre più solo sul proprio *core business* e affidare in outsourcing le attività secondarie.
Pertanto, seppur progettate come sistemi logicamente separati, produttori di servizi differenti, le infrastrutture, in particolare quelle definite critiche, sono diventate altamente interdipendenti, facendo ognuna affidamento (direttamente o indirettamente) su servizi forniti da altre. Tali connessioni contribuiscono a creare un enorme e complesso "sistema di sistemi", che appare estremamente incline a fenomeni di failure in cascata, come tristemente dimostrato dai black-out del 2003. In effetti, a causa della presenza di interdipendenze, un failure in ogni sottosistema può facilmente propagarsi agli altri, con il risultato di colpire un insieme di utenti vasto, imprevedibile e geograficamente distribuito.
Come esempio possiamo considerare il guasto nel 1998 del satellite delle telecomunicazioni Galaxy IV in orbita geo-stazionaria sulla west-coast degli Stati Uniti: si ebbero notevoli disservizi nelle comunicazioni (almeno il 90% dei cercapersone sono stati colpiti) e, inoltre, si manifestarono significative difficoltà anche

M. Aprile, S. De Porcellinis, R. Setola - Laboratorio Sistemi Complessi & Sicurezza, Università Campus Bio-Medico, Roma; S. Panzieri, Dipartimento di Informatica e Automazione, Università "Roma Tre"

nel sistema dei trasporti: molti voli subirono ritardi a causa dell'assenza delle informazioni sulle condizioni meteo in alta quota, mentre le operazioni di rifornimento sulle autostrade furono ostacolate dal fatto che le stazioni di rifornimento non furono più in grado di processare le transazioni delle carte di credito [2].
Un altro esempio interessante è quello dello scenario che si configurò nel gennaio 2004 quando si produsse un *failure* al sistema di condizionamento in un importate nodo di telecomunicazioni vicino Roma. Il guasto provocò in blackout delle telecomunicazioni via terra e wireless in un area estesa (colpendo tutti i fornitori del servizio), comportò la sospensione delle transazioni finanziarie in 5.000 banche e in 3.000 uffici postali e, addirittura disservizi nell'aeroporto internazionale di Fiumicino, dove circa il 70% delle postazioni per il check-in furono obbligate a ricorrere a procedure manuali [2].
In effetti, le infrastrutture critiche risultano estremamente vulnerabili a *failure* accidentali, come quelli provocati da fenomeni naturali, sempre più frequenti a causa della progressiva estremizzazione di alcuni eventi climatici. Per di più, tali infrastrutture possono diventare obiettivi di azioni terroristiche e criminali, data la loro crescente rilevanza. Attacchi portati contro queste infrastrutture creano danno, panico e diffidenza, potendo inoltre incrementare gli effetti dei più tradizionali attacchi terroristici (ad esempio rallentamento dei servizi di emergenza e ritardo nelle operazioni di salvataggio).
Queste considerazioni hanno spinto i governi e le organizzazioni internazionali ad attivarsi per migliorare la sicurezza, la robustezza e la resilienza di tali sistemi di infrastrutture. In particolare, lo scenario attuale impone la necessità di considerare, oltre a strategie settoriali per la sicurezza, anche la definizione di approcci coordinati e trasversali in grado di integrare in un unico framework i requisiti e i vincoli sulla sicurezza delle varie infrastrutture critiche. Simili specifiche strategie vengono usualmente indicate come CIP, Critical Infrastructure Protection, e CIIP, Critical Information Infrastructure Protection (quando l'attenzione è sulla componente ICT) [3].
Ovviamente, per sviluppare strategie di miglioramento delle prestazioni delle singole infrastrutture, sono indispensabili metodi e strumenti che consentano di capire e prevedere il comportamento globale del sistema di infrastrutture, anche quando esso operi in modalità degradata. Questa è una sfida non banale. Ogni infrastruttura critica è un *cluster* di sistemi che coinvogono anche operatori e utenti umani, complesso, altamente non lineare e geograficamente sparso. Ovviamente, la presenza di interdipendenze, molte delle quali nascoste o poco comprese, aumenta ulteriormente la complessità di questi sistemi, rendendo difficile l'applicazione degli standard e delle metodologie esistenti col fine di dedurne le caratteristiche strutturali, come i punti di equilibrio, la stabilità e, ancora più importante, il comportamento al transitorio.
In effetti, data la rilevanza del tema, in letteratura vengono sempre più frequentemente proposti approcci di analisi *ad hoc*, finalizzati in particolare ai sistemi di supporto alle decisioni, gestione dei rischi e migliore utilizzo delle risorse.
In questo articolo, illustreremo il progetto Cisia (Critical Infrastructure Simulation by Interdependent Agents), mirato a definire un approccio che, sulla base di informazioni principalmente qualitative, aiuti a inferire il comportamento complessivo del sistema [4].
L'articolo è organizzato come segue: nella sezione seguente, vengono brevemente presentati alcuni interessanti approcci proposti in letteratura per la modellazione, l'analisi e la simulazione di infrastrutture interdipendenti. Nella sezione *Linee guida per il disegno del simulatore* sono sintetizzate le caratteristiche chiave del nostro progetto. La sezione *Cisia* è dedicata alla descrizione dell'approccio proposto per modellare le interdipendenze e i comportamenti delle infrastrutture. La penultima sezione presenta un caso di studio e alcune note conclusive sono raccolte nell'ultima sezione.

Modellazione di infrastrutture interdipendenti

Procedure di modellazione e tecniche di simulazione per infrastrutture isolate sono ampiamente reperibili sul mercato, sotto forma di prodotti in grado di analizzare la singola entità a differenti gradi di astrazione, su scale temporali multiple e con un livello di dettaglio selezionabile.
Al contrario, la modellazione e la simulazione di infrastrutture multiple e interdipendenti è un settore ancora poco esplorato anche se conta un discreto numero di approcci in via di sviluppo. Questi (pochi) studi sono principalmente dedicati a determinare gli effetti in cascata, derivanti da uno più guasti all'interno di una singola infrastruttura in termini di estensione geografica dei danni, perdite economiche, altre infrastrutture affette ecc. In particolare, tali metodi si possono configurare quali utili strumenti per analizzare come le infrastrutture reagiscano a eventi estremi o rari, come i disastri naturali o gli attacchi terroristici. In effettti, data la rarità di questi eventi, e la grande e rapida innovazione che caratterizza lo scenario tecnico-sociale dei nostri tempi, i dati storici disponibili sono, troppo spesso, insufficienti per formulare ipotesi sul comportamento complessivo dei sistemi di infrastrutture in queste circostanze.
Nessuna simulazione, inoltre, può essere assolutamente predittiva e capace di ritrarre accuratamente le esatte conseguenze associate ad ogni singolo evento; tuttavia, le simulazioni possono aiutare a fornire utili input per lo sviluppo di iniziative di valutazione e gestione dei rischi, per piani di mitigazione e per strategie di protezione.
Alcuni tra gli approcci proposti sono estremamente qualitativi e principalmente orientati all'identificazione delle infrastrutture che devono essere considerate critiche, non in grado però di evidenziare il ruolo di ciascuna infrastruttura all'interno di un framework globale. Per esempio, il progetto Quick-Scan supportato dal governo olandese [5], era mirato a ottenere risposte alle seguenti domande: quali sono i settori, i prodotti e i servizi critici per l'Olanda? Quali sono i processi di fondo? Quali sono le (inter)dipendenze?
Le stesse questioni sono stata analizzate in [6], dove gli autori enfatizzano che nessuna delle definizioni date negli anni su cosa renda una infrastruttura "critica", possa essere considerata esaustiva: esse appaiono troppo ambigue e aperte a differenti interpretazioni. In [6] viene anche ribadito che, anche all'interno di uno stesso paese, la nozione di cosa viene considerato critico cambia nel tempo, e viene messo in evidenza come sia obbligatorio, in ogni caso, identificare i reali elementi critici all'interno delle dif-

ferenti infrastrutture.
Consideriamo, inoltre, che una rappresentazione puramente olistica di una singola infrastruttura rappresenti una semplificazione eccessiva, che non tiene conto della sua estensione geografica e della sua struttura. In [7] viene sottolineato come le interazioni tra componenti differenti producano la comparsa di comportamenti non direttamente deducibili dalla conoscenza delle caratteristiche di ogni singola componente. Questa condizione suggerisce di adottare approcci di tipo bottom-up, estremamente efficaci quando ci si confronta con informazioni di macro-scala scarse o mal definite, come accade ad esempio nella modellazione di fenomeni biologici e negli studi sulla bio-complessità.
In [8] è enfatizzato come, per comprendere correttamente il comportamento di queste infrastrutture, sia obbligatorio adottare un modello a tre strati: lo strato fisico, che contempla la componente materiale dell'infrastruttura, come ad esempio la griglia della rete elettrica; lo strato cyber, che include le componenti hardware e software dedicate a controllare e gestire l'infrastruttura (Scada e DCS); lo strato organizzativo, composto dall'insieme di procedure e funzioni usate per caratterizzare le attività degli operatori umani e per supportare la cooperazione tra le diverse infrastrutture.
In [8] gli autori enfatizzano che ogni componente di un'infrastruttura interagisce per mezzo di legami di inter-dipendenza, oltre che con gli elementi appartenenti alla medesima infrastruttura, anche con gli elementi delle altre infrastrutture presenti negli omologhi strati e, come la crescente presenza di questi legami determini numerose dipendenze funzionali. Inoltre, gli autori sottolineano quanto l'importanza dello strato cibernetico sia cresciuta negli ultimi dieci anni, divenendo uno dei più importanti fattori di interdipendenza. Si noti che una simile decomposizione è stata impiegata per analizzare il black-out che nel 2003 coinvolse gli Stati Uniti orientali e parte del Canada [9]. Come dato di fatto, per spiegare la moltitudine di cause che comportarono uno dei più estesi black-out della storia, le commissioni incaricate dal governo statunitense e da quello canadese descrissero gli eventi in termini di strati: la griglia di trasmissione (lo strato fisico), i computer e i sistemi di monitoraggio (lo strato cyber) e il fattore umano (lo strato organizzativo). Solo tenendo conto di tutti gli strati fu possibile comprendere come effettivamente si giunse al black-out.
Ancora più in dettaglio, in [7] gli autori enfatizzano come le interdipendenze dovrebbero essere analizzate rispetto a differenti dimensioni. In particolare essi catalogano le interdipendenze in quattro classi, non mutuamente esclusive:

- *Interdipendenza fisica.* Si realizza quando due infrastrutture sono fisicamente interdipendenti e quando le operazioni di una infrastruttura dipendono dall'output fisico di un'altra.
- *Interdipendenza cibernetica.* Presente quando lo stato di un'infrastruttura dipende dalle informazioni trasmesse o gestite da un'altra infrastruttura.
- *Interdipendenza geografica.* Si verifica quando gli elementi di più infrastrutture si trovano in prossimità spaziale.
- *Interdipendenza logica.* Due infrastrutture sono logicamente interdipendenti se lo stato di una dipende dallo stato dell'altra, tramite meccanismi di gestione, di regolazione o di altro tipo che non possono essere considerati fisici, geografici o cibernetici.

L'interdipendenza cibernetica è un fenomeno relativamente nuovo, strettamente correlato alla crescente dominanza dell'ICT e all'integrazione di sistemi di controllo computerizzati (ad esempio Scada) con altri sistemi informativi e ulteriormente esacerbato dall'uso di reti di comunicazione pubbliche. In [7] si sottolinea che l'interdipendenza cibernetica tende a essere una caratteristica assoluta e globale di tutte le infrastrutture, accoppiando potenzialmente ciascuna infrastruttura con ogni altra infrastruttura che usi il *cyberspace*, al di fuori della sua natura, tipo o ubicazione geografica, mentre altri tipi di interdipendenza risultano più locali e specifici. Incidentalmente, si noti che considerazioni di questo tipo suggeriscono ai governi e agli *stakeholder* la necessità di prestare particolare attenzione alle minacce provenienti dal *cyberspace* e in particolare a quelle che possono minare la "sicurezza" dei sistemi Scada esposti al *cyberspace* [10].
Un'altra prospettiva dalla quale analizzare il problema è fornita dall'analisi della topologia delle reti (di qualsiasi natura) e dallo studio di come questa ne influenzi la robustezza e le proprietà strutturali. I lavori pionieristici proposti da Watts e Strogatz [11] e da Albert et alii [12] enfatizzano alcune le peculiarità strutturali, mai evidenziate prima, comuni a molte reti e, tra queste, alle infrastrutture tecnologiche. Ad esempio, in [13] si sottolinea come la presenza di *hub* (nodi connessi con un gran numero di altri nodi) incrementi la robustezza rispetto ai guasti accidentali e, al tempo stesso, renda una rete estremamente vulnerabile ad attacchi mirati. Sebbene gli studi sul ruolo interpretato dalla struttura topologica all'interno di un *framework* di infrastrutture siano solo ad uno stadio preliminare [14] questi avranno, in futuro, una sicura rilevanza dal punto di vista analitico.

Linee guida per il disegno del simulatore

Un progetto di grande respiro sulla simulazione di infrastrutture critiche è attualmente in fase di sviluppo negli Stati Uniti, presso il Nisac (National Infrastructures Simulation and Analysis Centre). Questo centro, compartecipato dai laboratori Los Alamos e Sandia, è stato costituito nel 2001 con lo scopo di sviluppare metodi e strumenti per la modellazione e la simulazione delle infrastrutture ritenute vitali per gli Stati Uniti, unitamente alle interdipendenze esistenti tra loro. A tal fine, presso il Nisac si sta procedendo allo sviluppo di numerose suite software, basate su moduli interoperabili e capaci di supportare analisi estremamente dettagliate.
Ad esempio, la UIS (Urban Infrastructure Suite) è composta da sette moduli integrati, che impiegano avanzate metodologie di modellazione e simulazione delle infrastrutture urbane e della popolazione che le abita. Ognuno dei moduli che compongono la UIS adotta modelli molto dettagliati, come ad esempio il modulo Tass (Transportation Analysis Simulation System), il quale simula le attività quotidiane e gli spostamenti di cluster di individui statisticamente rappresentativi della popolazione presente in un'area urbana. Il Tass analizza le interazioni tra gli individui e le infrastrutture di trasporto, di telecomunicazione ecc., e può ad esempio prevedere, in presenza di un evento epidemiologico (come un attacco terroristico basato su agenti patogeni), come gli

spostamenti delle persone o i flussi di veicoli possano influenzare la diffusione epidemica.
Per realizzare tali strumenti, il Nisac e il governo statunitense stanno provvedendo alla raccolta di enormi quantità di dati riguardanti tutte le infrastrutture critiche presenti sul suolo nazionale, sfortunatamente però, sono disponibili pochi dettagli riguardo le attività e gli effettivi risultati ottenuti al Nisac.
È evidente che implementare modelli e simulatori come quelli sviluppati presso il Nisac risulta estremamente difficile, sia per il gap tecnologico che ci separa dagli Stati Uniti sia, soprattutto, per l'estrema difficoltà che si incontra nell'acquisizione di informazioni precise e dettagliate quando ci si interfaccia con gli stakeholder delle infrastrutture. Inoltre, è necessario, una volta ottenuti i dati di interesse, mantenerli continuamente aggiornati e allineati allo scenario reale, al fine di evitare i catastrofici effetti derivanti dalla produzione di previsioni incoerenti o fuorvianti.
Viste le precedenti considerazioni, abbiamo derivato alcune delle caratteristiche desiderabili per un simulatore di infrastrutture critiche, che tengano conto sia delle limitate risorse generalmente disponibili, sia della modesta "qualità" delle informazioni usualmente reperibili, in particolare:

- Ogni infrastruttura dovrà essere modellata decomposta nei suoi macro-componenti, cioè in oggetti con un ruolo specifico e facilmente riconoscibile secondo il livello di dettaglio richiesto. Il comportamento globale dovrà essere dedotto dalle interazioni tra dette macro-componenti.
- Per ridurre il fabbisogno di informazioni dettagliate, ogni elemento dovrà essere definito con un livello di astrazione sufficientemente alto, tale da consentire la formulazione di modelli consistenti e verosimili, basandosi sui dati, spesso generici o frammentari, acquisibili dagli *stakeholder* e dai documenti di pubblico accesso.
- La rappresentazione "esterna" di tutte le macro-componenti dovrà essere uniforme, per facilitare la formulazione dei modelli e la codifica delle interfacce.
- Parametri e variabili saranno codificati utilizzando numeri *fuzzy*. In questo modo, non solo sarà possibile codificare affermazioni vaghe quali "il componente B dipende molto dal componente A", ma, anche, analizzare i risultati di una simulazione in termini di affidabilità e precisione.
- Le descrizioni delle macro-componenti dovranno essere indipendenti e auto-contenute. Le dinamiche di ciascuna macro-componente dovranno fare riferimento solamente a parametri interni e a valori esplicitamente scambiati con altri blocchi.
- Il simulatore non dovrà imporre limitazioni di sorta, riguardo i comportamenti rappresentabili, per consentire agli esperti di ciascun dominio la massima capacità di espressione possibile.

Ci siamo quindi ispirati a questi principi di base per formulare un metodo di modellazione adatto a catturare i comportamenti più significativi delle infrastrutture critiche, a partire da informazioni frammentate, disomogenee e ambigue.
Ogni infrastruttura viene decomposta nelle sue macro-componenti, allo scopo di trasformarla in un cluster di vari elementi interconnessi, in numero dipendente dalla scala spazio/temporale adottata e dal livello di dettaglio richiesto.
Ogni macro-componente viene caratterizzata dalla capacità di eseguire correttamente il compito per il quale è stata creata, ovvero di produrre determinate quantità di beni o servizi, e dal suo livello di failure (considerando le differenti tipologie di guasti ai quali può andare incontro, ognuna con un livello arbitrario di severità).
Essendo interessati ad analizzare il comportamento di intere infrastrutture in presenza di attacchi o malfunzionamenti indotti, si trascurano le dinamiche fisiche interne (che supponiamo essere adeguate in situazioni normali) mentre si adotta una descrizione basata su disponibilità di risorse (beni o servizi necessari al corretto funzionamento di ciascuna macro-componente) e livelli di guasto (che inficiano il corretto funzionamento dei vari elementi). In tal modo si modellano le interazioni tra le macro-componenti facendo riferimento allo scambio di limitati insiemi di grandezze, le risorse e i guasti dai quali dipende la capacità operativa di ciascuna macro-componente. Si noti che la necessità di considerare diverse tipologie di guasto è mandatoria, dato che, come spiegato in dettaglio nella sezione successiva, ciascuna tipologia è caratterizzata da fenomeni di diffusione differenti e può incidere in maniera diversa sull'operatività di ciascuna macro-componente.
Ciascuno scenario, quindi, viene descritto in termini di n macro-componenti, caratterizzate dallo scambio di p tipi di risorse e m tipologie di guasti. Per ciascun tipo di risorsa o guasto si considerano specifici meccanismi di distribuzione o diffusione facendo riferimento a differenti concetti di prossimità.

Cisia

Usando le precedenti considerazioni, è stato implementato un framework di simulazione, Cisia (Critical Infrastructure by Interdependent Agents), atto ad analizzare propagazione di guasti e degradazione delle performance di un sistema composto da infrastrutture differenti, eterogenee e interdipendenti.

Modellazione e dinamica delle macro-componenti
Ogni macro-componente è modellata come un blocco autonomo (di seguito chiamato "entità") il cui comportamento è descritto, almeno, dalle seguenti quantità:

- *Livello Operativo* (OL): rappresenta la capacità dell'entità di eseguire il suo lavoro. Rappresenta solo la capacità "potenziale", ovvero, un livello operativo del 100% non significa che il sistema stia effettivamente lavorando alla sua massima capacità, ma che potrebbe farlo se necessario. Questa quantità può variare nel tempo in un intervallo di valori compreso tra zero e uno e ogni condizione anomala di funzionamento è caratterizzata da un livello operativo inferiore all'unità. Il livello operativo, come tutte le altre grandezze utilizzate nel simulatore, è rappresentato da un numero fuzzy.
- *Failure* (F): è una variabile strutturata, che enumera i tipi di guasti interni che possono colpire l'entità e memorizza il livello attuale di severità associato a ciascun tipo. Mentre le tipologie tipi di guasto rappresentano una proprietà statica di ciascuna entità, i livelli di severità associati possono aumentare in determinate situazioni (si noti che i livelli di severità non possono diminuire dal momento che abbiamo escluso dall'analisi procedure di *fixing*).
  Il livello di severità di ciascun tipo di guasto è rappresentato da

una grandezza normalizzata, nell'intervallo [0,1], dove 0 rappresenta l'assenza del guasto e 1 il massimo livello raggiungibile.

Ogni entità è caratterizzata, inoltre, da un insieme di parametri costanti, utilizzati per specificare con maggior dettaglio le sue caratteristiche funzionali. Alcuni dei parametri più frequentemente utilizzati sono: *Requisiti* (REQ) che specificano tipi, unità di misura e valore delle *Risorse* necessarie a raggiungere un livello operativo pari al 100%; *Livello di Produzione Nominale* (NPL), una variabile strutturata che indica quale siano le risorse prodotte dall'entità e in che quantità vengono prodotte quando l'entità è caratterizzata da un livello operativo del 100%.

Le entità interagiscono attraverso lo scambio delle seguenti quantità:

- *Risorse* (R): beni e servizi prodotti (o usati) dall'entità, espressi in termini del loro tipo, unità di misura, valori nominali e livelli reali. Si noti che, come per il livello operativo, le Risorse scambiate tra due entità non rappresentano l'effettivo ammontare di beni prodotti, ma le quantità massime che l'entità può produrre se necessario. Si assume che l'*i*-esima entità produca e richieda, rispettivamente, p_i e r_i differenti tipi di risorse (dove numero e tipi dipendono dalla caratteristica dell'entità).
- *Consumi* (C): risorse effettivamente usate dall'entità, espresse in termini dei loro tipi, unità di misura, valori nominali e quantità. Queste quantità vengono scambiate tra le entità che utilizzano le risorse e quelle le producono, vengono usate per stimare effetti di saturazione o condizioni di sovraccarico.
- *Failure* (F): guasti propagati da (o verso) le entità, espressi in termini dei loro tipi e dei livelli di severità associati. Si assume che l'*i*-esima entità possa essere affetta da m_i differenti tipi di guasti (dove numero e tipi dipendono dalla caratteristica dell'entità).

Si noti che, per migliorare l'efficienza della simulazione, riducendo la formazione di pericolosi anelli di feedback, le interazioni tra le entità sono basate sullo scambio di grandezze che rappresentano le massime quantità di risorse "producibili", anziché i livelli di produzione effettivi. Infatti, anche se si è adottato un paradigma che prevede un produttore e un consumatore, questi risultano, comunque, parzialmente disaccoppiati. Il consumatore opera sulle capacità potenziali del produttore, mentre quest'ultimo è completamente indipendente dalle richieste del consumatore, fintanto che i consumi effettivi non inducano fenomeni di sovraccarico.

Il Livello Operativo di ciascuna entità è pari al 100% quando sono assenti guasti interni (F) e le risorse disponibili (R_{IN}) risultano maggiori o uguali ai requisiti dell'entità (REQ). Il Livello Operativo dell'entità può quindi diminuire progressivamente all'aumentare dei livelli di guasto interni e al diminuire delle risorse disponibili. Quando OL=0 l'entità non è in grado di fornire alcuna risorsa, anche se può ancora generare e/o trasmettere guasti. In particolare:

$$OL_i = \prod_{k=1}^{m_i} \{\Lambda_k [F(k)]\} * \prod_{j=1}^{h} \Theta_k \left[\frac{REQ(j)}{R_{IN}(j)}\right] \qquad (1)$$

dove Λ e Θ assumono valori nell'intervallo [0,1], Λ_k è una funzione decrescente (con $\Lambda_k(0) = 1$), Θ_j è una funzione crescente (con $\Theta_j(1) = 1$).

Λ e Θ possono appartenere alle classi, illustrate nella figura 1 o a loro combinazioni pesate. Si noti che funzioni lineari (a) e a soglia (b) sono genericamente più facili da configurare, anche se il miglior fitting con i dati sperimentali si ottiene, in genere, con l'impiego delle funzioni logistiche (c).

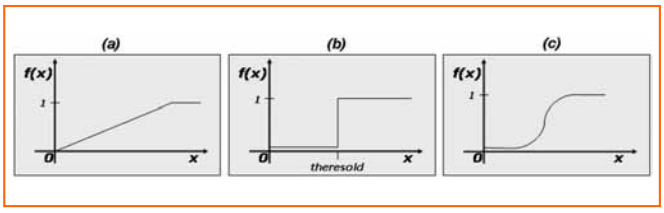

Figura 1 - Classi di funzioni utilizzate nei modelli delle entità

Le risorse prodotte dalle entità sono, in genere, sempre proporzionali al Livello Operativo, mentre il consumo di risorse può dipendere sia dal Livello Operativo che dai consumi provenienti da altri elementi, cioè

$$C_{OUT} = \Omega(OL, C_{IN}, NSL) \qquad (2)$$

dove NSL specifica il *Livello di Produzione Nominale*, un valore di riferimento che rappresenta l'ammontare di risorse che l'entità può fornire con un OL pari al 100%.

Nel caso in cui un'entità riceva un guasto di tipo *X* che possa condizionarne in qualunque modo la dinamica interna, essa aggiorna il suo stato interno secondo:

$$F(X) = \Psi_X \{ F(X), \Delta(F_{IN}(X)), C_{IN} \} \qquad (3)$$

dove ψ_X è la funzione che determina come un livello di guasto interno sia influenzato dai guasti provenienti dall'esterno, dagli eventuali sovraccarichi o dai guasti già presenti all'interno dell'entità; Δ è la funzione che modifica la severità del guasto ricevuto, in accordo con il profilo di resilienza dell'entità.

A loro volta, i guasti interni possono generare guasti in uscita dall'entità (F_{OUT}), che possono quindi diffondersi alle entità vicine in accordo con il concetto di prossimità associato al tipo di guasto.

Modellazione delle interdipendenze

Particolare attenzione è stata riservata al metodo di modellazione delle dipendenze e interdipendenze tra le varie macro-componenti, essendo queste la principale causa della complessità emergente dei comportamenti di tali sistemi. Ogni macro-componente interagisce con le altre tramite una moltitudine di meccanismi. Tra questi, quelli legati a dipendenze di tipo funzionale sono, di solito, noti e facilmente caratterizzabili, perchè concepiti o volontariamente realizzati dai progettisti dei vari sistemi. Tipicamente, infatti, è attraverso tali legami funzionali che gli elementi e i le componenti di una infrastruttura scambiano tra di loro i prodotti o i servizi.

Tra i meccanismi di interazione che si realizzano tra le componenti delle infrastrutture è possibile, però, individuarne alcuni, identificati in genere come *legami indiretti* [15], che non essendo stati volontariamente pianificati o implementati sono spesso la conseguenza di fortuita o casuale di determinate tipologie di pros-

➤

simità tra gli elementi di un sistema. A volte, tali legami indiretti, non esistono in condizioni di funzionamento normale, ma si manifestano come conseguenza di specifici guasti, peculiari condizioni operative o cambiamenti del contesto nel quale le infrastrutture operano.
Di seguito, per evidenziare la differente natura dei legami di tipo funzionale da quelli di tipo indiretto, si farà riferimento ai primi come ai link di scambio delle Risorse, attraverso cui le entità scambiano le risorse necessarie al loro funzionamento, mentre i secondi saranno costituiti dai legami di propagazione dei Failure, attraverso i quali si possono propagare i guasti.
Per entrambe le categorie, comunque, si devono considerare differenti meccanismi di propagazione, ognuno caratterizzato da differenti topologie e metriche, considerando per ciascuna macro-componente insiemi distinti di entità adiacenti.
In Cisia gli scambi di grandezze tra le macro-componenti hanno luogo mediante lo scambio di messaggi, realizzato secondo i cammini orientati descritti all'interno di differenti matrici di adiacenza, ognuna delle quali dedicata alla descrizione di un determinato concetto di prossimità
Inoltre, ciascun termine all'interno delle matrici di adiacenza è composto da due coefficienti rispettivamente, il guadagno e il ritardo che interessano le grandezze veicolate attraverso il link descritto dal termine (cfr figura 2).

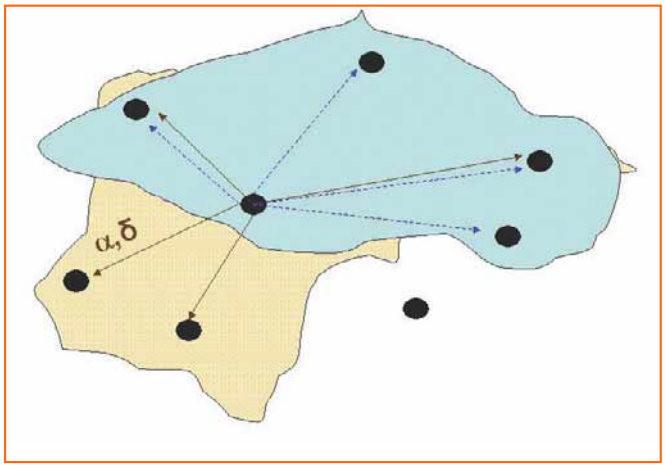

Figura 2 - Individuazione degli elementi di adiacenza del nodo centrale rispetto a due differenti concetti di prossimità (line continua e linea tratteggiata)

L'uso di differenti tipi di matrici, al di là di porre enfasi sulle differenti caratteristiche di ogni concetto di prossimità, semplifica notevolmente l'individuazione delle interdipendenze. Seguendo la tassonomia introdotta in [7] possiamo affermare che: le interdipendenze fisiche sono, generalmente, ben conosciute agli esperti delle infrastrutture e spesso sono immediatamente deducibili dagli schemi funzionali/di progetto; le interdipendenze geografiche, benchè meno conosciute, possono essere scoperte confrontando le mappe delle infrastrutture; le interdipendenze di tipo logico, in ultimo, sono le più ostiche da identificare e, purtoppo, rappresentano la principale causa dei fenomeni in cascata.
Per quanto riguarda la propagazione dei guasti, l'approccio proposto introduce una distinzione diffusione e propagazione. Ogni guasto viene diffuso a tutte le entità adiacenti a quella che lo ha

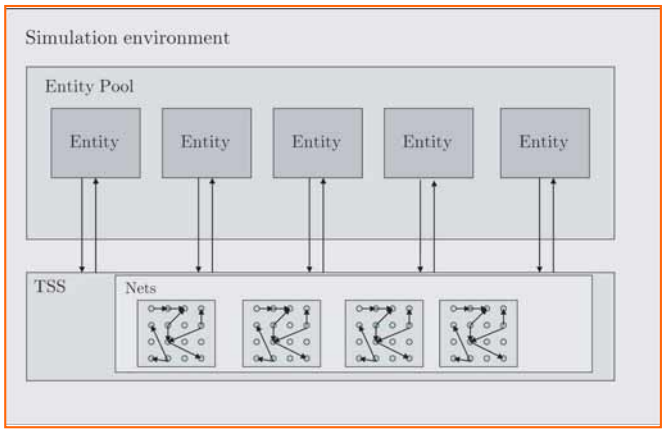

Figura 3 - Il simulatore è composto da due strutture principali: l'Entity Pool, che gestisce la dinamica interna di ciascuna entità e il Transmission Sub System (TSS), che ha il compito di gestire le diverse interazioni fra le entità

prodotto ma viene propagato (ovvero modifica effettivamente lo stato o le dinamiche dell'entità) solamente alle entità che, sulla base del loro profilo di resilienza, gli risultano vulnerabili.

Funzionamento del simulatore
Ciascuno scenario è caratterizzato in termini di entità e di matrici di adiacenza. Entità e matrici sono contenute e gestire da due strutture, rispettivamente Entity Pool (EP) e Transmission Sub System (TSS), mostrati nella figura 3.
Il TSS è dedicato a gestire la comunicazione tra le entità. Le entità comunicano tramite scambio di messaggi, dove ogni messaggio contiene dati circa il tipo e la quantità denormalizzata di risorsa (o guasto) trasportata, il coefficiente di normalizzazione, l'unità di misura e l'identificativo del mittente. Quando il TSS riceve il segnale dal clock di simulazione, raccoglie i messaggi in uscita da tutte le entità e inoltra ogni messaggio ai vicini dell'entità mittente, in accordo con le adiacenze descritte nella matrice associata con il tipo di quantità trasportata. Se un link tra due entità adiacenti è caratterizzato da fattori di attenuazione o di ritardo il TSS provvede a ritardare la spedizione del messaggio instradato su quel link e a scalare appositamente le quantità trasportate.
All'arrivo del segnale di clock, l'EP calcola, per ogni entità, il livello operativo e i livelli di guasto sulla base delle grandezze che l'entità ha ricevuto in ingresso. Successivamente, in base ai valori delle variabili stato, l'EP calcola l'ammontare delle risorse e dei guasti prodotti da ciascuna entità, che vengono poi inviati al TSS affinché siano propagati ai diversi insiemi di entità vicine.

Caso di studio

Uno dei test effettuati con Cisia ha riguardato l'analisi delle possibili conseguenze di un guasto all'interno di uno degli impianti elettrici demandati alla produzione di elettricità per l'area di Roma.
Lo scenario è stato modellato apportando notevoli semplificazioni rispetto al caso reale, ricercando, più che l'ottenimento di previsioni realistiche, conferma delle effettive potenzialità della metodologia e del simulatore Cisia nello studio di uno scenario

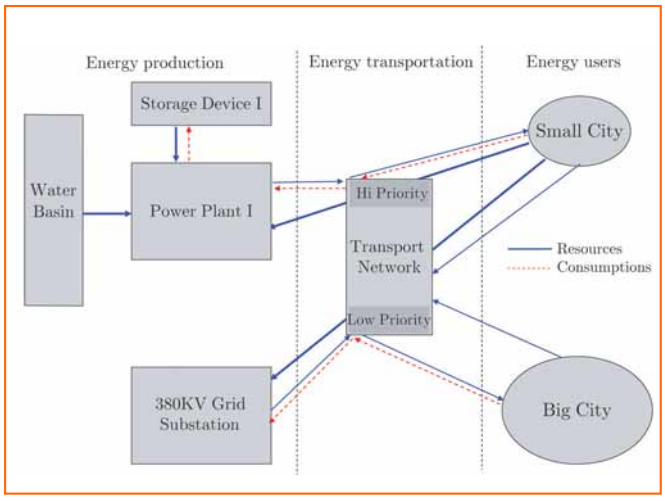

Figura 4 - Lo scenario analizzato: una schematizzazione semplificata dell'infrastruttura elettrica della zona di Roma

'verosimile' pur se non esattamente coincidente con uno scenario reale.
Lo scenario in esame comprendeva 6 tipologie di entità differenti, afferenti a diverse tipologie di infrastrutture, in particolare:

- *Power Plant:* un generico centro di produzione elettrica localizzato vicino all'area urbana di Roma. Questa entità modella un insieme di impianti termoelettrici geograficamente colocati nella stessa area (che condividono risorse comuni come riserve di carburante e sistema di raffreddamento dell'acqua).
- *Storage device:* il gruppo di strutture e sistemi che garantiscono la fornitura di carburante verso il Power Plant.
- *Water basin:* il bacino di invaso che fornisce acqua agli impianti di generazione.
- *380 kV Grid Substation:* il punto di contatto tra la rete di trasmissione nazionale e quella presente nell'area in esame. Anche se nell'area di Roma sono presenti diversi punti di interconnessione con la rete di trasmissione nazionale, visto il livello di dettaglio generale si assume la presenza di un unico punto.
- *Transport Network:* è la rete, con l'associato sistema di telecomunicazione e telecontrollo, che distribuisce elettricità alle aree urbane.
- *Small/Big cities:* due aree urbane vicine e di differenti dimensioni. Big City rappresenta una città, mentre Small City un'area sub-urbana. Seppure la reale architettura usata per la supervisione e il controllo della rete di trasmissione elettrica sia estremamente complessa, contemplando la presenza di numerosi centri di controllo locali coordinati da un nodo nazionale, abbiamo assunto che all'interno della Small City fosse presente il centro di controllo demandato alla gestione degli impianti di produzione, trasmissione e distribuzione di energia elettrica presenti nello scenario.

Semplificando, si assume che, per poter generare elettricità il Power Plant abbia bisogno di ricevere carburante, acqua e informazioni di controllo. Inoltre, si assume che il fabbisogno di energia elettrica delle aree urbane sia tale da rendere indispensabile l'energia prodotta dal Power Plant locale. A valle del Power Plant e della 380 kV Grid Substation è collocata la Transport Network, che riceve elettricità da queste ultime e garantisce l'approvvigionando di energia alle aree urbane. Si assume che, il livello operativo delle aree urbane dipenda direttamente dall'adeguata disponibilità di energia elettrica; quando un black-out colpisce le aree in questione si verifica, a seconda della durata e della gravità, la degradazione di alcuni servizi di base (trasporti, telecomunicazioni, gestione delle emergenze ecc.) che, specie se prolungata, può indurre condizioni di pericolo o disagi gravi alla popolazione. Si suppone, inoltre, che il sistema di gestione della Transport Network adotti una politica di priorità tale da privilegiare nella fornitura di elettricità la Small City, dove risulta collocato il centro di controllo della griglia elettrica.
In una delle simulazioni effettuate, abbiamo supposto che all'istante T=20 un incendio improvvisamente renda inservibili le riserve di carburante presenti nello Storage Plant (cfr figura 5.a).

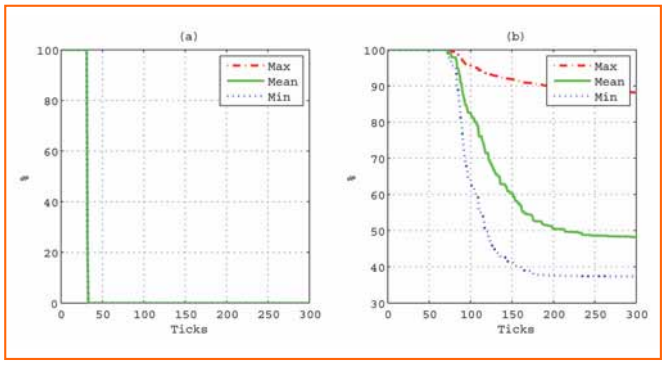

Figura 5 - OL associato con il Power Plant (a) e con la 380 KV substation (b). Tutte le grandezze sono rappresentate mediante numeri fuzzy triangolari

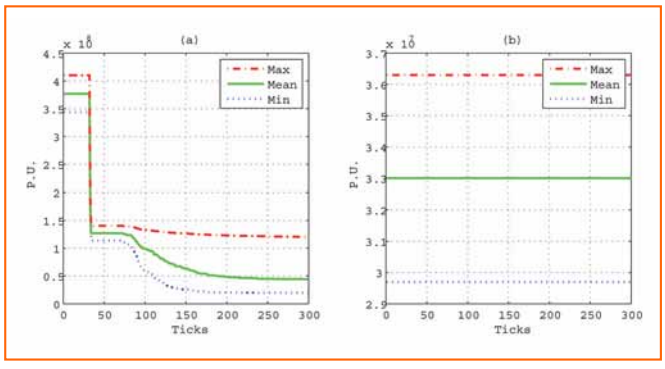

Figura 6 - Energia elettrica a disposizione della Big City (a) e della Small City (b). Tutte le grandezze sono rappresentate mediante numeri fuzzy triangolari

Anche se la 380 kV Grid Substation continua a fornire elettricità (cfr figura 5) questa, venendo a mancare l'apporto del Power Plant, non risulta sufficiente a soddisfare le esigenze delle aree urbane. In accordo con la politica di dispacciamento definita la Transport Network riduce la fornitura di energia verso la Big City, connessa a una linea a bassa-priorità (cfr figura 6.a), nell'intento di garantire un apporto costante alla Small City, connessa ad una line ad alta priorità .
L'ammanco di energia, dopo un certo tempo, induce disservizi nella Big City che, di conseguenza, vede il suo Livello Operativo ridursi progressivamente (cfr figura 7.a).

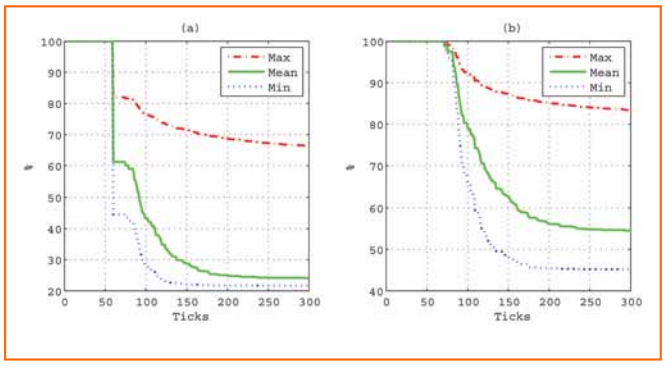

Figura 7 - OL associato con la Big City (a) e con la Small City (b). Tutte le grandezze sono rappresentate mediante numeri fuzzy triangolari

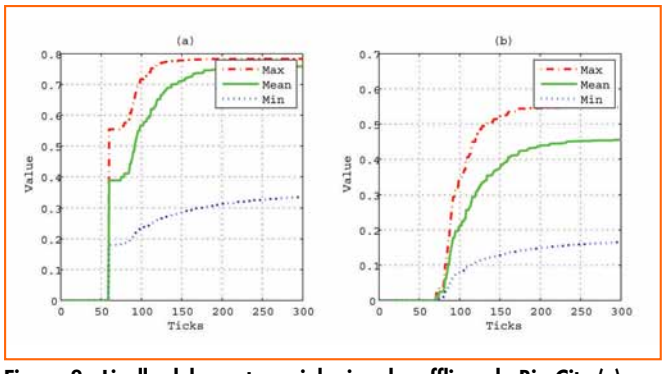

Figura 8 - Livello del guasto sociologico che affligge la Big City (a) e la Small City (b). Tutte le grandezze sono rappresentate mediante numeri fuzzy triangolari

Dato l'impiego dei numeri *fuzzy* per la codifica delle varie grandezze, si possono individuare, sui grafici temporali relativi a ciascuna grandezza, tre curve: la curva centrale (continua) rappresenta il comportamento più "credibile", mentre quella superiore (tratteggiata) e quella inferiore (punteggiata) rappresentano,a seconda del caso, una stima del caso migliore e di quello peggiore. Oltretutto, l'impiego della codifica f*uzzy* consente di caratterizzare l'incertezza o l'imprecisione associata ai dati ottenuti, che, in un dato istante, risultano proporzionali alla distanza tra il massimo e il minimo valore assunto dalla variabile *fuzzy*.
Osservando la figura 7.b, si può notare come, dopo alcuni istanti, pur non essendoci stata alcuna riduzione della corrente fornita alla Small City, quest'ultima cominci a soffrire una degradazione del proprio Livello Operativo.
Tale comportamento è dovuto alla propagazione di un failure di tipo 'sociologico' generatosi all'interno della Big City. Il black-out indotto nella grande area urbana, infatti, produce la degradazione di alcuni servizi critici (blocco dei trasporti su ferro, congestione del traffico, difficoltà nella comunicazione, problemi nella sanità e nei servizi d'emergenza ecc.) e induce disturbi che, data la supposta prossimità geografica delle due aree, si propagano alla Small City andandone a inficiare la capacità operativa (cfr figura 8.b).
La presenza di tali disturbi ha quindi un impatto sulla capacità del centro di controllo, presente nella Small City, di gestire in maniera efficiente la griglia di trasmissione a 380 kV (cfr figura 5). Questo esaspera ulteriormente la condizione di black-out nella Big City e, ovviamente, incrementa il livello di failure sociale. Si innesca così un fenomeno a catena che, dopo un periodo di transitorio, porta ad una nuova condizione di equilibrio del sistema.
A regime, infatti, si può notare come, nonostante la Small City rimanga continuamente alimentata, il suo livello operativo risulti ridotto a circa il 40% del suo livello nominale. Tale risultato suggerisce che nello scenario (molto semplice) analizzato , la politica di distribuzione adottata dalla Transport Network risulti scarsamente efficace e suggerisce la necessità di sperimentare strategie differenti.

Conclusioni

L'articolo descrive un approccio per modellare le interdipendenze tra infrastrutture, con il fine di effettuare un'analisi di impatto catturando alcuni fenomeni significativi. Questo approccio, implementato in un simulatore pienamente operativo (Cisia), è stato ideato per tenere conto di diversi meccanismi di interdipendenza e per consentire una gestione di informazioni dotate di un certo grado di incertezza. Questi ultimi elementi risultano piuttosto rilevanti in uno scenario che comprenda delle infrastrutture in quanto le informazioni a disposizione sono spesso scarse, ambigue e soggettive, sia in termini di analisi delle interdipendenze, sia per la loro affidabilità intrinseca. Si dimostra importante, inoltre, l'allineamento dei dettagli di modellazione alla qualità dei dati disponibili. Per superare parzialmente questo svantaggio, si è proposto di adottare una rappresentazione astratta delle infrastrutture in termini della loro capacità di produrre beni e servizi sulla base della disponibilità di risorse esterne, tenendo conto della presenza (e severità) di differenti tipi di guasti. Il comportamento globale del sistema è quindi ottenuto considerando l'instradamento e la diffusione tra i macro-componenti delle varie risorse e degli eventuali guasti. In questo modo è stato possibile adottare un framework standard per modellare varie classi di macro-componenti, facilmente scalabili per adattare meglio la granularità delle informazioni disponibili. Inoltre, per gestire meglio l'ampia incertezza che caratterizza queste classi è stato suggerito di rappresentare le differenti quantità tramite i numeri *fuzzy*.
Cisia, oltre a fornire uno strumento di simulazione, supporta anche l'analisi topologica sui differenti scenari. Ovviamente, una piena analisi topologica su un ambiente pesantemente multi-stratificato come un framework di più infrastrutture, può non risultare completa. Tramite Cisia si è in grado di scoprire sia gli effetti di un dato guasto sull'intera rete di infrastrutture, sia come un dato guasto si propaghi attraverso i differenti strati di interdipendenza. Vengono evidenziati quali nodi rappresentano i punti deboli rispetto ad una certa classe di guasti/attacchi o come la combinazione di eventi concorrenti possa contribuire a rendere peggiore uno scenario già critico.
Infine, la possibilità di utilizzare differenti matrici di adiacenza, permette all'analista di descrivere in modo semplice uno scenario complesso, dove alcuni elementi sono legati insieme tramite relazioni multiple. Un compito assai arduo da portare avanti con un approccio monolitico.
Ulteriori sviluppi di questo lavoro consisteranno nel costruire una raccolta di blocchi per gli elementi più comuni delle infrastrutture

importanti, e nell'implementazione di un'interfaccia utente adatta a rendere più intuitiva la codifica dei comportamenti dei macro-componenti, al fine di testarlo su differenti scenari.

Bibliografia

[1] E.U. Commission Communication, "Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection", *Com(2006)787*. Brussels, 2006.

[2] Gruppo di Lavoro per la Protezione delle Infrastrutture Critiche Informatizzate, *La Protezione delle Infrastrutture Critiche Informatizzate*, La Realtà Italiana, 2004.

[3] M. Dunn, I. *Wigert, International CIIP Handbook*, ETH, The Swiss Federal Institute of Technology, Zurich, 2006.

[4] S. De Porcellinis, S. Panzieri, R. Setola, G. Ulivi, "Simulation of Heterogeneous and Interdependent Critical Infrastructures", *Int. J. Critical Infrastructure* (IJCI) (in stampa).

[5] A. Luiijf, H. Burger, H. Klaver, "A Critical (information) Infrastructure Protection in The Netherlands" *In Proc. Critical Infrastructure Protection* (CIP) Workshop, Frankfurt, Germany, 2003.

[6] J. Moteff, C. Copeland, J. Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical?" In *Report for Congress RL31556*, The Library of Congress, 2002.

[7] S. Rinaldi, J. Peerenboom, T. Kelly, "Identifying Understanding and Analyzing Critical Infrastructure Interdependencies", *IEEE Control System Magazine*, pp. 11 - 25, 2001.

[8] R. Macdonald, and S. Bologna, "Advanced Modelling and Simulation Methods and Tools for Critical infrastructure Protection". Technical report. ACIP project report, 2001.

[9] U.S. and Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, 2004.

[10] U.S. Government, *The National Strategy to Secure Cyberspace*, The White House, Washington, USA, 2003.

[11] D. Watts, S. Strogatz, "Collective dynamics of 'small-world' networks", *Nature*, 393, pp. 440 - 424, 1998.

[12] R. Albert, H. Jeong, A. Barabasi, "Error and Attack Tolerance of Complex Networks", *Nature*, 406, pp. 378-382, 2000.

[13] R. Albert, A. Barabasi "Statistical Mechanics of Complex Networks", *Reviews of Modern Physics*, 74, pp. 48 - 97, 2002.

[14] S. De Porcellinis, L. Issacharoff, S. Meloni, V. Rosato, R. Setola, F.Tiriticco, "Modelling interdependent infrastructures using interacting dynamical models", *Int. J. Critical Infrastructure* (IJCI) (in stampa).

[15] R. Benoit, "A Method For The Study Of Cascading Effects Within Lifeline Networks". *Int. Journal of Critical Infrastructure*, 1, pp. 86 - 99, 2004.